



UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,364	07/17/2003	Colin John Blamires	03.028.01	8923
<div><div>7590</div><div>05/15/2007</div><div>Zilka-Kotab, PC P.O. Box 721120 San Jose, CA 95172-1120</div></div>				
			<div>EXAMINER</div> <div>SIMITOSKI, MICHAEL J</div>	
			<div>ART UNIT</div> <div>2134</div>	<div>PAPER NUMBER</div>
			<div>MAIL DATE</div> <div>05/15/2007</div>	<div>DELIVERY MODE</div> <div>PAPER</div>

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,364	BLAMIRE ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 March 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,7-11,15-19 and 23-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,7-11,15-19 and 23-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 March 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 3/12/2007 was received and considered.
2. Claims 1-3, 7-11, 15-19 & 23-31 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-3, 7-11, 15-19 & 23-31 have been considered but are moot in view of the new ground(s) of rejection. However, applicable arguments are given below.

4. Applicant's response (p. 10, last paragraph) argues that the firewall limitations of claims 5, 13 & 21 have a limiting effect on the claim. However, regarding for example claim 1, the claim is directed to a removable physical media comprising a computer program that loads network support code from the removable physical media, where the network support code is used to enable said computer to establish a secure network connection via a firewall computer to a remote computer. The limitation recited that a firewall is disposed between the computer being controlled by the removable physical media and the remote computer appears to have no limiting effect on the removal physical media itself. At most, the only tie between the firewall and the removable physical media in the claim is such that the media comprises network support code to enable the computer to establish the claimed secure connection via the firewall; one of ordinary skill in the art knows that since a firewall operates on packets, the only requirement this limitation places on the claim is that the network support code supply some form of communication packets. The packets encountering the firewall, much less specifically traversing the firewall, is a system limitation involving the firewall, having no effect on the removable

physical media. The same response is submitted regarding claim 9; claim 9 is directed to a method, where the method is not affected by the firewall, its operation or its position. The same response is submitted regarding claim 17; claim 17 is directed to a computer, where the computer is not affected by the firewall, its operation or its position. The same response is submitted regarding claim 25; claim 25 is directed to a server, where the server is not affected by the firewall, its operation or its position. Further, regarding claim 25, the following limitations appear to have no effect on the claim:

- i. “wherein said computer is booted with a non-installed operating system read from a removable physical media instead of an installed operating system stored on said computer”
- ii. “wherein network support code is loaded for said computer read from said removable physical media”
- iii. “wherein malware detection is performed upon said computer using said one or more malware detection files”.

The above limitations are in question because the claim is directed to a server computer and the above limitations appear to provide no further components of the server computer.

Further, regarding claim 31, the limitation “wherein said remote computer logs said downloading of said one or more malware detection files by said computer” appears to have no effect on the claim because claim 1 is directed to a removable physical media which does not necessarily change as a result of the actions of a remote computer. As a result, the limitation “wherein a firewall computer ... other than said secure connection” and the limitations listed in

this section are not given patentable weight. However, for the purposes of the rejections based on art in this action, to expedite prosecution, the above limitations are addressed.

5. Applicant's response (p. 12) argues that the reference does not disclose "loading network support code for said computer read from said removable physical media". However, Reinert explicitly discloses a bootable virus utility program loaded from a storage medium (col. 6, lines 55-56) that comprises a communications program (col. 6, line 60) that is used to connect to a remote computer (col. 7, lines 4-5).

6. Applicant's response (pp. 12-13) argues the inherency reasoning given in the first action. As new grounds of rejection are necessitated by Applicant's amendments, it is noted that the limitation "wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer other than said secure network connection" does not limit the claim, as described above. Further, the limitation "is operable to block a connection" limits "firewall" only to the extent that the firewall has the ability to block a connection, which is what firewalls inherently do.

7. In light of Applicant's amendments, the Stallings reference is submitted. Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and

the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer (pp. 320-323). As stated above, the network support code (communications program of Reinert) is already used to enable the computer to establish a connection (secure connection, as modified by Yadav) to said remote computer. As herein modified, the code is also used to establish the secure connection via said firewall, as the packets must traverse the firewall for reception at the remote computer.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-3, 7-11, 15-19, 23-25 & 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,347,375 to Reinert et al. (**Reinert**) in view of U.S. Patent Application Publication 2003/0149887 to **Yadav** and Network Security Essentials, Applications and Standards by **Stallings**.

Regarding claim 1, Reinert discloses a removable physical media (CD-ROM, col. 6, line 66) bearing a computer program (bootable virus utility, col. 6, lines 55-56) operable to control a computer to detect malware (viruses) by performing the steps of booting said computer with a

Art Unit: 2134

non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media(CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28), and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (§42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, §42) over a VPN or SSL connection to safeguard the updates (§§43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been

Art Unit: 2134

motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 2, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 3, Reinert discloses wherein said steps further comprise loading security management code (communications program, col. 7, lines 65-67) operable to control said downloading (col. 8, lines 20-25).

Regarding claim 7, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 8, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 9, Reinert discloses booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28) and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (§42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, §42) over a VPN or SSL connection to safeguard the

updates (§§43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (§§42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 10, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 11, Reinert discloses wherein said steps further comprise loading security management code (communications program, col. 7, lines 65-67) operable to control downloading (col. 8, lines 20-25).

Regarding claim 15, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 16, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 17, Reinert discloses a computer (computer 42, col. 7, line 60), said computer comprising a processor (CPU, col.6, lines 39-40) performing the steps of booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25) , performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28) and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of

than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer". However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (§42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, §42) over a VPN or SSL connection to safeguard the updates (§§43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (§§42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer

security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 18, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 19, Reinert discloses wherein said steps further comprise loading security management code (communications program, col. 7, lines 65-67) operable to control said downloading (col. 8, lines 20-25).

Regarding claim 23, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 24, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 25, Reinert discloses a server computer (remote computer 54, col. 8, lines 10-11) connected by a network link to a computer (computer 42, Fig. 2), said server computer comprising a processor (inherent) configured to perform the steps of establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), loading one or more malware (virus) detection files (col. 8, lines 20-25) to said computer, wherein said computer is booted with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from a removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, wherein network support code (communications program) is loaded for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), wherein said network support code (communications program, col. 7,

lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said server computer (col. 7, lines 4-5 & lines 65-67), wherein malware detection is performed upon said computer using said one or more malware detection files (virus definition files, col. 8, line 10-11 & line 28). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (§42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, §42) over a VPN or SSL connection to safeguard the updates (§§43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (§§42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in

Art Unit: 2134

a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 28, Reinert discloses wherein said remote computer (remote computer 54) determines said one or more malware detection files that are downloaded to said computer (downloaded under the control of remote computer 54, col. 8, lines 10-25).

Regarding claim 29, Reinert discloses wherein said one or more malware detection files are determined based on said non-installed operating system (the malware detection files and service program must be able to run on the booted operating system, col. 8, lines 14-16 & lines 25-31).

Regarding claim 30, Reinert discloses wherein said one or more malware detection files (virus detection signature file) are determined based on a malware detection product (the virus detection signature file is used by the virus scanning software utility program, col. 8, lines 20-35).

Art Unit: 2134

10. Claims 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Reinert, Yadav and Stallings**, as applied to claim 1 above, in further view of U.S. Patent 6,721,883 to Khatri et al. (**Khatri**).

Regarding claim 26, Reinert lacks wherein said computer is configured in its BIOS settings. However, Khatri teaches that computer systems boot from a specific device (col. 1, lines 16-17) by scanning through a boot order (col. 1, lines 35-39) that is determined by a BIOS setup routine (col. 4, lines 15-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to configure the BIOS settings to boot from said removable physical media. One of ordinary skill in the art would have been motivated to perform such a modification to allow a modern computer system to boot from the CD-ROM of Reinert, as taught by Khatri (col. 1, lines 16-17, lines 35-39 & col. 4, lines 15-17).

Regarding claim 27, Reinert lacks wherein booting said computer with said non-installed operating system read from said removable physical media is based on a determination that a bootable removable media is present. However, Khatri teaches that computer systems boot from a specific device (col. 1, lines 16-17) by scanning through a boot order (col. 1, lines 35-39) such that the system attempts each device in a specific order (i.e. determines if each device can be boot from and boots from the first available, col. 1, lines 35-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Khatri to base the booting the computer with said non-installed operating system on a determination that the removable media is present. One of ordinary skill in the art would have been motivated to perform such a modification to use a standard computer boot order to boot

Art Unit: 2134

from Reinert's CD-ROM, as taught by Khatri (col. 1, lines 16-17, lines 35-39 & col. 4, lines 15-17).

11. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Reinert, Yadav and Stallings**, as applied to claim 1 above, in further view of U.S. Patent U.S. Patent 2003/0028889 to McCoskey et al. (**McCoskey**).

Regarding claim 31, Reinert lacks wherein said remote computer logs said downloading of said one or more malware detection files by said computer. However, McCoskey teaches a content delivery system such that when content is downloaded to a client, a delivery server logs the download so that billing servers can determine if the user will be charged a fee (§126).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert's remote computer such that it logs the downloading of one or more malware detection files. One of ordinary skill in the art would have been motivated to perform such a modification to allow a billing server to charge a fee for the download, as taught by McCoskey (§126).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. U.S. Patent 7,171,692 to DeMello et al. is cited for teaching logging a download from a server for the purposes of billing (col. 12, lines 44-60).

Art Unit: 2134

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

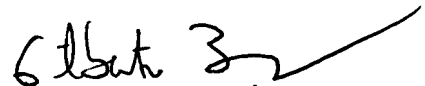
Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS



May 9, 2007



GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100